GET STRAIGHT IN THE HAIGHT

CHESS BARBS

NWLF ATTACK IN BERKELEY

Berkeley Barb

VOL. 20, NO. 18, ISSUE 483, NOVEMBER 15-21, 1974
2042 UNIVERSITY AVENUE, BERKELEY, CA 94704, UG9-1040
PUBLISHED EVERY FRIDAY 204
Copyright: Berkeley Barb 1974
25c Bay Area 50c Elsewhere

THE IBM PAPERS

The document reproduced on these pages was obtained for the Berkeley Barb by the New York News Service.

IBM

INTERNATIONAL BUSINESS MACHINES

AND

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

POLICE

Security: A Management Style
A Course of Instruction in Corporate Protective Services

IBM AS A TARGET FOR TERRORISTS

BIBLIOGRAPHY

Bremer, Arthur H. *An Assassin's Diary*, New York: Harper's Magazine Press, 1973.

"Kinshasa, Kwando" (pseud. for William Ernest King, Jr.) *Urban Warfare*, Gaithersburg, Md.: International Association of Chiefs of Police Clandestine Tactics and Technology Service Terrorist Document Reprint, 1974.

Marighella, Carlos. *Minimanual of the Urban Guerrilla*, : "New World Liberation Front U.S.A.", 1970.

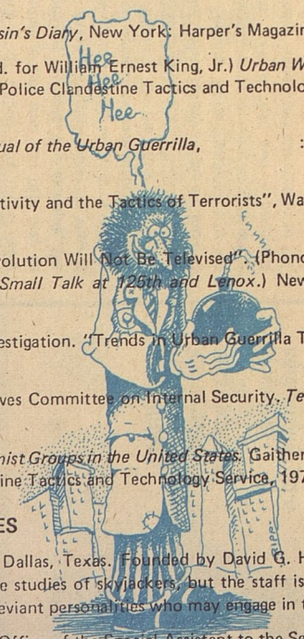
Methvin, Eugene H. "Objectivity and the Tactics of Terrorists", Washington *Star-News*, February 24, 1974, p. F-2.

Scott-Heron, Gil. "The Revolution Will Not Be Televised". (Phonograph record, with title band based on selection from author's *Small Talk at 125th and Lenox*.) New York: Flying Dutchman Productions, Ltd., BDL 1-0613, 1974.

U.S. Federal Bureau of Investigation. "Trends in Urban Guerrilla Tactics". *FBI Law Enforcement Bulletin*, July, 1973, pp. 1-5.

U.S. House of Representatives Committee on Internal Security. *Terrorism: A Staff Study*. 93rd Cong., 2nd Sess., August 1, 1974.

Vestermark, S. D., Jr. *Extremist Groups in the United States*. Gaithersburg, Md.: International Association of Chiefs of Police Clandestine Tactics and Technology Service, 1974.



GENERAL RESOURCES

Aberrant Behavior Center, Dallas, Texas. Founded by David G. Hubbard, M.D., the Center specializes in conducting intensive case studies of skyjackers, but the staff is available for consultation on particular problems presented by deviant personalities who may engage in terrorist acts.

U.S. Department of State, Office of the Special Assistant to the Secretary and Coordinator for Combatting Terrorism, Washington, D.C. The primary overt Government mechanism for assembling and disseminating information on terrorist activities and counter-terror measures. Provides special briefings on world-wide conditions.

PRINCIPLES: The Spectrum of Real Terrorist Threats Against IBM (continued)

-3-

SABOTAGE

ESPIONAGE

"HIT" TACTICS

SOUTH AFRICA AS AN INCREASINGLY CRITICAL AREA

In both relatively less and relatively more industrialized societies, IBM may expect acts of *sabotage*. It may experience terrorist *espionage* against its trade secrets and, indeed, it may find that terrorists *overtly* strike at certain laboratory and office locations, both to seize trade secrets and technology, and to assault "American overseas imperialism". In view of the political changes now taking place in the buffer states around the Union of South Africa, security planners must view this region as especially sensitive during the mid-1970's. Here, a complex set of forces is at work to endanger the assets of the Western businessman and his own personal safety. Not only are economic and political control centers relatively concentrated, and thus susceptible to urban guerrilla tactics, but the emergence of effective Black nationalism means that Black majorities now will demand substantial control over in-place business assets. Those who resist may find themselves simply expropriated when Black nationalists come to power. Prior to taking power, Black nationalist and terrorist groups may selectively target Western business interests which they view as especially symbolic of the oppression they are seeking to eliminate.

CRITICAL OVERSEAS AREAS

In short, South America, the Middle East, and certain areas of Africa are likely arenas for continued large-scale terrorism against American businessmen. Relatively more developed areas which are closely linked by communications to these areas can expect sabotage, espionage, and other limited strike tactics, under the direction or influence of main line terrorist organizations or their overseas affiliates. Western Europe and Japan continue to be areas likely to be subject to these more limited terrorist strike tactics.

IN THE UNITED STATES

In the United States. Domestically, IBM can expect more limited attack by terrorists and extremists. Nevertheless, there are specific points which should be of continuing concern to security managers.

RADICAL EXTREMIST INTEREST IN IBM

For the domestic *radical extremist*, IBM remains as a symbol of post-industrial technological oppression, which is vulnerable both because of its general role in technology and because it is a strong, relatively self-contained organization which has successfully resisted unionization. Radical activists can be expected to follow the litigation against IBM with much interest, both to verify their own perceptions that it is a monolithic trust, and to search for specific points on which the Corporation can be pressured and penetrated.

THE NCLC

Beyond various bombing incidents for which the Weather Underground and residues of the Venceremos Organization may try to take credit, likely specific radical efforts will center on attempts to organize and manipulate IBM workers. One group which may be increasingly active is the National Caucus of Labor Committees. Alleged operatives of the NCLC have distributed copies of *New Solidarity*, the NCLC's newspaper, at at least one

U.S. Federal Bureau of Investigation, Office of the Director, Washington, D.C. Specialized resources and non-classified information briefings, upon appropriate request.

U.S. House of Representatives Internal Security Committee, Washington, D.C. A hard-working staff assembles a broad range of materials on extremism and terrorism, some of which are available through Staff Reports, Hearings, and other vehicles of dissemination.

PRINCIPLES: Image and Reality as Seen by Terrorists

IBM'S RELATIVELY FORTUNATE EXPERIENCE TO DATE

Unlike other organizations of similar scope, such as Exxon, Ford, and ITT, IBM has to date been spared many of the more dramatic acts of terrorists. While IBM has had to address a problem of bomb threats and arson, its employees have not yet been kidnapped or murdered, and other acts of assault, extortion, and duress have been relatively limited in impact. Of course, one of the reasons for IBM's relatively fortunate experience is that it has had a relatively low profile in some of the overseas areas where major terrorist groups currently operate. In addition, its domestic labor policies appear to have had some effect in dampening the kinds of discontents which create the internal turmoils that make an organization attractive for meddling by outsiders. IBM may also simply have been lucky. Luck ought not be discounted, especially when it is remembered that among domestic campus radicals of the mid-1960's, a number of whom have since gone underground to continue their organizing work, IBM was synonymous with an "oppressive system" which, they said, "folded, spindled, and mutilated" *them*. Looking now at what terrorists and extremists have done during the first five years of the 1970's, it is probable that the future will be less benign for IBM.

THE TERMS "TERRORIST" AND "EXTREMIST"

The terms "terrorist" and "extremist" are, for most practical purposes, interchangeable, although "terrorist" tends to connote the application of violence to *individuals* or *institutional symbols* in order to advance the cause of a *clandestine political* movement. (See the historical overview of the term "terrorist" provided in House Internal Security Committee Staff Study, 1974, pp. 5-8.) One definition of "extremist group" (Vestermark, 1974, p. 1), prepared for analyzing domestic American cases, holds that

A DEFINITION OF "EXTREMIST GROUP"

> An extremist group is a group which, operating beyong legal constraints, plans and executes violence or threats of violence against persons and property, as a strategy for achieving political, social, cultural, or economic objectives.

THE CRITICAL ROLE OF THREATS AND ACTS OF VIOLENCE

Even in the domestic American setting, where the words and nonviolent but coercive symbolic gestures of extremists have often been as important as their acts of violence, the threat of violence has given their efforts that critical cutting edge, which is intended to intimidate and coerce their opponents.

WHAT VIOLENCE AND THREATS OF VIOLENCE CAN ACCOMPLISH

Extremists and terrorists may have major internal disputes about whether actually to use violence, or what the proper overall role of violence ought to be in their organizations. All seem to sense, however, that violence and threats of violence accomplish many things for them. Not only do they create excruciating psychological torment in those who must respond, but they generate a very particular "scapegoat" effect. A sustained campaign of violence and threat often works to make the target – the established institution, organization, or system – somehow "responsible" in the public eye for the suffering created by the violence. An ideologically and tactically adroit terrorist group can push establishment organizations into over-reaction, and by avoiding capture, make it appear as if the establishment groups are the ones responsible for initiating and perpetuating the violence. The establishment group becomes both the victim of the terrorists and the lightning rod upon which the larger public can discharge its frustrations over the continuing uncertainty and fear. When the public begins scapegoating the *victims* of terrorism, then terrorism becomes truly a formidable weapon – especially if the terrorists manage to articulate genuine grievances.

THE "SCAPEGOAT" EFFECT

IBM Site, and it is probable that there is NCLC interest in IBM at other locations. The central theme of the less paranoid component of NCLC propaganda is that conventional trade unions are ineffective and dying – and that local labor committees which organize, direct, and reflect a real *political mass movement* among the working class are the needed alternative. As the editorial in the July 10, 1974 *New Solidarity* declares, in part (p. 11),

PRINCIPLES: The Spectrum of Real Terrorist Threats Against IBM (continued)

NCLC STRATEGY, AS SUGGESTED IN AN EDITORIAL FROM *NEW SOLIDARITY*

> r you say, "There's no way a strike can win", and the workers shrug, giving a look that implies you have failed his test, how do you judge this pathological reaction by these workers?
>
> In fact, those workers are reacting like the proverbial goldfish dumped into a large pool after being raised in a small bowl. Although they have contempt for existing unions, they continue to swim in small-trade union mentality-circles. They will probably agree that political organization is necessary ("Yeah, sure, I'm going to vote for you guys in the election"), but they will still insist, "Our problem is to figure out some way to win a strike". They refuse to see that strikes will become effective again only when they are local actions by a mass-based *political* organization. They are slow to see only because, like the proverbial goldfish, they do not yet see the larger domain of political action as an area in which they can actually swim.
>
> The great, suicidal danger among the ten thousand-odd hard core of our North American readers is the tendency to make some concession to the continuing goldfish tendencies among the majority of militants. As long as you try to "win friends and influence people" among these workers by catering to old trade-union-action illusions, you are disorienting them by postponing the day on which they begin to conceptualize real political organization and tactics.
>
> The key to the future is to take a stubborn position for the necessary policy today, even if that appears – temporarily – to be a very unpopular position. Our policy toward the mass of working people must be: We know what to do. When you guys wise up and decide to listen to us on this, we'll all begin to accomplish something".

Earlier in the same statement, the editorialist specifically attacks both "labor bureaucrats" and "silly Communist Party militants mouthing the current party line". In the place of these outmoded failures, the editorial holds out the prospect of truly effective Labor Committees, who will move the workers directly into the political power struggle.

THE TROTSKYITE AND PROGRESSIVE LABOR VIEW

Those who know the internal schisms of the Communist movement recognize this thinking as derivative of the Trotskyite and Progressive Labor view of political action. In real terms, it means that non-union workers may be especially interesting for "politicalization" by NCLC, because there is no pre-existing union infrastructure to block or impede the process. Evidences of increasing radical-led political activity within a specific labor force include work slow-downs, active disruption and sabotage, and non-negotiable demands on non-wage issues, such as day care centers for dependents, women's and minority rights, use of drugs, and the general conditions of labor. Note, however, that while extremist tactics may be used to advance these demands, there may be little initial overt use of terror. Instead, organizers will seek to build political momentum, with which management must deal, and to which they must ultimately make more basic concessions on the structure and nature of the business itself.

EVIDENCES OF RADICAL ATTEMPTS TO "POLITICIZE"

RADICAL "TIGHT COLLECTIVES" AS A MAJOR THREAT OF VIOLENCE

The skilled radical extremist organizer recognizes that terror tactics can quickly backfire against him, particularly if one of the "working class" gets hurt. For this reason, it is more likely that acts of terroristic violence or kidnapping will continue to come from small radical anarchist "tight collectives" (see the discussion in Vestermark, 1974, pp.

see next page

PRINCIPLES: Countermeasures

-5-

64-69), who act out their fantasies through violence and who basically disregard the safety of others – including "workers", who may turn out to be merely "unfortunate" sacrifices to the violent act. Monitoring the activities of these tight collectives is a major challenge to law enforcement as well as to corporate intelligence units, since they are difficult to penetrate and often ephemeral, changing from one group into another as the fantasies of their members change.

RESTORATIONIST EXTREMISTS, AND POSSIBLE INTERESTS IN IBM

For the domestic *restorationist extremist*, IBM is only rarely likely to be a target. Main line American restorationists are likely to be proud of IBM as a symbol of American strength, although Minutemen and Birchers will be alarmed at evidences of IBM's dealing with Soviet Bloc countries and the People's Republic of China. The more likely restorationist attack on IBM will come from those small groups who fear IBM may be doing something to compromise very specific, immediate interests. For example, the Jewish Defense League claims to remain ready to attack – through guerrilla theater tactics, bombings, arson, and acts of sabotage directed against technical systems – those who support enslavers of Soviet Jewry. Banking and oil companies have special need for precautions against JDL tactics, but IBM may not be immune. On the other side of the coin, white supremicist groups will always be attracted to organizations which have racial conflict, or which appear to be catering to the "Jews" who, racists allege, are inciting "Negroids". Neo-Nazi groups such as the National Socialist White People's Party are currently much more interested in "forced school busing" controversies than they are in looking for racial turmoil in business organizations. Yet, if IBM ever experiences particular incidents of racial conflict, or if it must make some overt concession to the JDL, then it can be expected that the NSWPP and other white racist groups will come scampering, to see what mischief can be stirred.

COUNTERMEASURES

COUNTERMEASURES

A FUNDAMENTAL DANGER

DANGERS OF COVERT TACTICS

Countermeasures to terrorism and extremism contain a fundamental danger – that in seeking to block terror tactics, those in control of the countermeasures will lapse into the same tactics. True, some situations may call for the application of limited covert strike tactics. But these tactics must be governed by law and be under the control of duly appointed law enforcement agents. Even then, they are dangerous, in that their use can create a "garrison state" psychology within an organization, where the tactics of "secret warfare" become self-perpetuating and endlessly fascinating. Americans have had numerous recent reminders of the pitfalls that await those who become enthralled by the covert response.

What, then, can be done about possible acts of terrorism and extremism against IBM? Options available will certainly vary, according to whether the response must be made domestically or overseas, and according to the scale of the terrorist act. In general, however, certain basic principles should govern the development of a Corporate response to terrorism.

PRINCIPLES: Develop an Effective Intelligence System on the Plans and Acts of Extremists and Terrorists

-6-

DEVELOP AN EFFECTIVE INTELLIGENCE SYSTEM ON THE PLANS AND ACTS OF EXTREMISTS AND TERRORISTS

DEVELOP AN INTELLIGENCE SYSTEM

The more violent and dangerous the terrorist tactic, the more necessary will be surprise in its execution. It is absolutely critical to any response that this surprise component be reduced, and that the organization have timely, comprehensive intelligence information on likely threats.

An intelligence system on terrorists and extremists should allow rapid acquisition, analysis, and dissemination of current data from a specially constituted, specially skilled group, which exists in close liaison with top management. Among the information with which this group would work would be:

INFORMATION NEEDED FOR THE INTELLIGENCE SYSTEM

– general traits and methods of groups likely to be threats;

– detailed, timely incident reports on all events of terrorism and extremism and all events which may have been stimulated or supported by terrorist groups;

– the content of specific threats, including blackmail-extortion and bomb threats, in a format designed to examine for basic data trends in threat data;

– points of potential vulnerability of key corporate figures and key corporate locations, with projected hypothetical assaults against them;

– projected possible response scenarios.

THE PAP

The group would be equippe
should be staffed to provide
for specific situations. It sh
actual response.

CENTRALIZE AND COORD
AND EXTREMISM, WITHOU
FLEXIBILITY AT THE LOC

COORDINATE RESPONSES, THROUGH AN "ACTION DIRECTORATE"

EXAMPLE: RESPONDING TO A KIDNAPPING

Terrorists and extremists see
successfully engaging in the "
work at cross purposes and
Further, they seek to use
response. Responses before
the organization on the terr
may be necessary to engage
appear to be negotiating on
Corporate figures and their f
the mass media, and to be o
leave the hostage. If the g
effective action against the t
prospect of success.

PRINCIPLES: Have Multiple, Flexible Respons For a Variety of Contingencies

-7-

RESPONSIBILITIES OF THE "ACTION DIRECTORATE"

Corporate countermeasures sho
can function both at CHQ le
inventory of both policies an
should be in continuing coord
recognition of the fact that te
organizations, but vulnerabiliti
plan and act in concert.

HAVE MULTIPLE, FLEXIBLE
VARIETY OF CONTINGENCI

HAVE MANY RESPONSE OPTIONS

The Corporation should know
types of situation:

OPTIONS NEEDED FOR AT LEAST THESE TYPES OF SITUATION

– persistent bomb threats;

– possible sabotage of its techn

– kidnap/hostage and coercive

– blackmail attempts at extorti

– group assaults on its Sites;

– agitation intended to disrupt

Some requirements and opti
systematically explored, using
to do so.

RESPONDING TO A KIDNAPPING

Consider the possible respons
immediately critical. Should t
and technical information, no
attempted with the kidnapp
location of the hostage unkno
are holding him barricaded i
should be available to partic

IBM
ERS

d to issue periodic as well as special intelligence alerts, and it analytic support in developing immediate countermeasures uld thus be in close relation to those who must make the

INATE THE RESPONSE TO TERRORISM
IT DESTROYING NECESSARY TACTICAL
AL LEVEL

k to demonstrate the vulnerability of an organization by propaganda of the deed", while elements of the organization in conflict, as they attempt to develop a timely response. tealth and speed, before the organization can make any r after-the-fact to terrorists should focus all the resources of rists. For example, if a kidnapped hostage is being held, it n a variety of covert and overt tactics – simultaneously, to ansom, to be searching for the victim, to be protecting other amilies, to be engaging in effective public relations through pening up "zones of safe return", in which the abductors can als are (1) to get the victim back safely, and (2) to take rrorists, then only careful coordination can provide any real

se Options

uld be under the control of an "action directorate", which vel and as a flexible resource to Sites. It should have an d systems, for the range of likely response situations. It ination with similar directorates in other organizations, in rrorists seek to exploit vulnerabilities of not only specific es created by the failure of *organizational communities* to

E RESPONSE OPTIONS FOR A
IES

what its response options are for at least these general

nology;

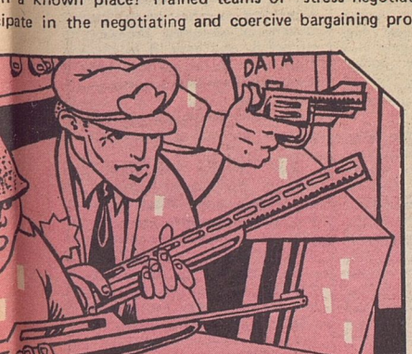
bargaining situations;

ion;

work and to set management against other personnel.

ions may be clearer than others, but all should be simulation and gaming techniques when possible and useful

ses to kidnapping. Naturally, the question of ransom is he Corporation pay? Suppose the demand is for technology t money. What ought to be done? Should bargaining be ers? How does the bargaining situation vary, when the wn, contrasted with the situation in which the kidnappers n a known place? Trained teams of "stress negotiators" ipate in the negotiating and coercive bargaining process.



But – their actions must be closely coordinated with the actions of others in the action directorate. Furthermore, Corporate actions may need to proceed simultaneously with covert or overt law enforcement actions. Mechanisms for this coordination must exist prior to actual kidnap experience.

THE LACK OF STABLE DOCTRINE ON RESPONDING TO TERRORISM

The latent message of these questions is that there is, as yet, no real "book" on kidnapping or on most other potential acts of terrorism. This is partly because of severe limitations on what private organizations can do, and it is certainly a reflection of wide differences among corporate philosophies on how best to meet terrorists and extremists. Consequently, IBM faces a major task in defining and analyzing its own multiple response options.

PRINCIPLES: Maximize the Inherent Weaknesses of Terrorists and Extremists

-8-

MAXIMIZE THE INHERENT WEAKNESSES OF TERRORISTS AND EXTREMISTS

MAXIMIZE THE WEAKNESS OF TERRORISTS

In spite of their impact and glamor for some, the acts of terrorists and extremists contain a fundamental weakness. This is the simple fact that many people do not want to live by terror. Thus, it is critical that counter-terror operatives minimize the use of terror tactics themselves, and that they work hard to avoid becoming the public's scapegoat for what terrorists themselves have created.

MARIGHELLA'S "SEVEN SINS OF THE URBAN GUERRILLA"

Beyond this general strategic consideration, Marighella himself acknowledges "The Seven Sins of the Urban Guerrilla" (Marighella, 1970, pp. 38-39). Consider each one in turn.

1. INEXPERIENCE

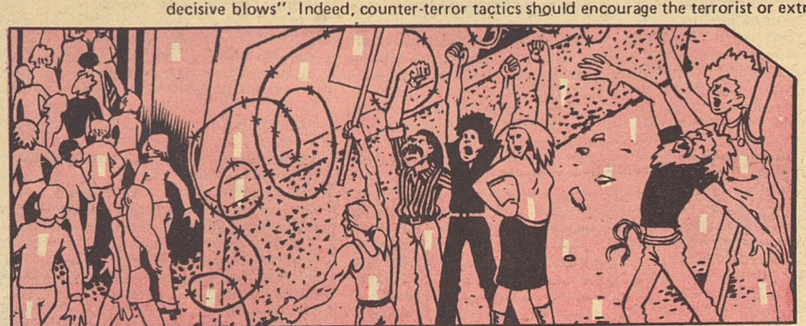
"The first sin of the urban guerrilla is inexperience" – thus he misjudges situations, thinks the opposition is stupid, overestimates the enemy, leaves clues, and lacks audacity. Obviously, counter-terror tactics can contribute in a number of ways to continuing to make the guerrilla vulnerable to his own inexperience and his own incorrect estimates and judgments.

2. BOASTFULNESS

"The second sin of the urban guerrilla is to boast about the actions he has completed and broadcast them to the four winds". Counter-terror clandestine operatives, if skillfully placed, can encourage the guerrilla and extremist to commit this sin.

3. VANITY

"The third sin of the urban guerrilla is vanity. . . . Blinded by success, he winds up organizing an action that he considers decisive and that puts into play all the forces and resources of the organization. Since the city is the area of the strategic circle which we cannot avoid or break while rural guerrilla warfare has not yet erupted and is not at the point of triumph, we always run the fatal error of permitting the enemy to attack us with decisive blows". Indeed, counter-terror tactics should encourage the terrorist or extremist



to expose his full organization, by full commitment to a given situation.

4. TO EXAGGERATE STRENGTH

"The fourth sin of the urban guerrilla is to exaggerate his strength and to undertake projects for which he lacks forces and, as yet, does not have the required infrastructure". Consider the effects, for example, of a skillful media campaign in causing the terrorist to overestimate himself and to commit himself prematurely, thus opening up pre-emptive strike possibilities.

5. PRECIPITOUS ACTION

"The fifth sin of the urban guerrilla is precipitous action". How can counter-terror operatives induce just such precipitous, unprepared action?

6. TO ATTACK WHEN ANGRY

"The sixth sin of the urban guerrilla is to attack the enemy when he is most angry". Indeed – this illustrates the enduring value of the right kind of *provocateur*.

PRINCIPLES: Maximize the Inherent Weaknesses of Terrorists and Extremists (continued)

-9-

7. TO FAIL TO PLAN

"The seventh sin of the urban guerrilla is to fail to plan things, and to act out of improvisation". Continuing pressure applied to terrorists and extremists can make improvisation – and the resulting frustration and disorganization – a continuing necessity for self-styled "urban guerrillas".

THE SEVEN SINS DO NOT, HOWEVER, IMPLY A FULL COUNTER-TERROR STRATEGY

Marighella's list of sins does not, when turned on its head, constitute a strategy for attacking the urban guerrilla. But it does tell much about the inherent vulnerabilities of terrorists. Properly guided and focused, counter-terror activities can encourage guerrillas to sin by their own standards, to create a continuing record of their true selves – as small, willful bands of extremists, who use terror to deprive both individuals and lawful groups of the basic human values of personal safety and personal integrity.

Continued Next Week